

POLÍTICA DE SEGURIDAD DE PROVEEDORES

El Centro de Conciliación – Junta de Prevención y Resolución de Disputas & Arbitraje JC, en adelante **CRA – JC** - establece esta política con el propósito de garantizar la seguridad de la información y los servicios de procesamiento de información a los cuales tienen acceso a terceros, entidades externas o que son procesados, comunicados o administrados por estos.

Antes de iniciar la ejecución de contratos con terceras partes, se deben suscribir los respectivos acuerdos de confidencialidad, los cuales deben incluir:

- Cláusulas de confidencialidad, asegurando la protección de la información.
- Compromisos en materia de seguridad de la información, aplicables durante y después de la vigencia del contrato.

Asimismo, se deben establecer mecanismos de control en las relaciones contractuales para garantizar que:

- La información a la que tengan acceso los proveedores cumpla con las políticas de seguridad y privacidad de la información de la organización.
- Los servicios provistos por los proveedores cumplan con los estándares de seguridad establecidos.

Las políticas de seguridad de la organización deben ser difundidas por los funcionarios responsables de la elaboración y/o firma de contratos o convenios con proveedores.

Por otro lado, los contratos o acuerdos con los proveedores deben incluir una cláusula de terminación en caso de incumplimiento de las políticas de seguridad y privacidad de la información.

En este sentido, la organización ha definido las siguientes cláusulas:

1: Acuerdo de confidencialidad

1.1: El acuerdo de confidencialidad debe ser firmado, sin excepción, por cualquier proveedor con el que se establezca un intercambio de información.

1.2: Este acuerdo debe estipular que el acceso a los datos vinculados al servicio prestado

a la organización solo podrá ser realizado por personas y/o entidades formalmente autorizadas.

1.3: Debe incluir penalizaciones basadas en los daños potenciales derivados de la violación de la confidencialidad de la información.

2: Protección de datos personales

2.1: Se debe incluir en el acuerdo de confidencialidad con el proveedor una cláusula que establezca el cumplimiento de la Política de Protección de Datos Personales de la organización.

2.2: El documento de la política debe ser entregado al proveedor para su comprensión y aceptación formal.

3: Requerimiento de Seguridad de Aplicaciones y/o Servicios

3.1: Si el proveedor es responsable de aplicaciones o servicios informáticos, estos deben cumplir con los requerimientos de protección de la confidencialidad, integridad y disponibilidad, definidos por la organización. Dichos requerimientos deberán ser demostrados en función del activo que será gestionado, mediante uno o más de los siguientes controles:

- **Monitoreo:** El proveedor debe contar con mecanismos que permitan detectar incidentes de seguridad de la información en la aplicación utilizada para la prestación del servicio. El nivel de detección debe ajustarse a los requerimientos del activo involucrado.
- **Control de acceso:** Se deben presentar mecanismos de control de acceso a los servicios y datos manejados, en cumplimiento de la PO-13 Política de Control de Acceso. El acceso a la información de la organización por parte de proveedores debe limitarse estrictamente a lo necesario para cumplir con el servicio asignado.
- **Gestión de incidentes:** El proveedor debe notificar inmediatamente a la organización sobre cualquier incidente de seguridad de la información o ciberseguridad que pueda afectar los activos tecnológicos de la organización y/o sus clientes, ya sea directa o indirectamente.
- **Licenciamiento:** Todas las aplicaciones y servicios prestados por el proveedor deben contar con licencias vigentes, en conformidad con el marco legal y regulaciones aplicables.

- **Cumplimiento de Políticas:** Las personas que actúan como proveedores de la organización deben seguir las Políticas de Seguridad y Privacidad de la Información. Como excepción, en caso de incumplimiento, el proceso disciplinario se gestionará bajo la figura de incumplimiento de contrato.

3.2: Las obligaciones de confidencialidad continuarán vigentes incluso después de la finalización del contrato por cualquier causa.

3.3: La organización se reserva el derecho de realizar auditorías extraordinarias, siempre que existan causas justificadas.

3.4: El proveedor debe comunicar oportunamente a la unidad orgánica usuaria del servicio cualquier cambio en el personal asignado a la prestación del servicio.

4: Prohibiciones del Proveedor (a)

4.1: Usar los recursos proporcionados por la organización para actividades no relacionadas con el propósito del servicio.

4.2: Intentar y/u obtener, sin autorización explícita, otros derechos o accesos distintos a los que la organización haya asignado.

4.3: Intentar y/o acceder, sin autorización explícita, a áreas restringidas de la organización.

4.4: Revelar, modificar, destruir o dar mal uso a la información a la que tenga acceso.

4.5: Utilizar la información de la organización para beneficio propio o de terceros.

4.6: Realizar copias no autorizadas de software, en cumplimiento de la Ley sobre el Derecho de Autor.